Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application.

Please amend claim 1, 13, 18 and 27 as indicated below (material to be inserted is in **bold and underline**, and material to be deleted is in ~~strikeout~~ or (if the deletion is of five or fewer consecutive characters or would be difficult to see) in double brackets [[ ]]).

Listing of Claims:

1. (Currently Amended) A method of encrypting an image produced from physical information, comprising:

digitizing spatially-distributed physical information to create a digital image of the information;

digitizing a physical tag associated with the physical information to create a digital tag, the digital tag being readable to identify a public key **that is a public member of an asymmetric public-private pair of cryptography keys**;

reading the digital tag to identify the public key; and

encrypting the digital image with the identified public key.

2. (Original) The method of claim 1, further comprising physically associating the physical tag with the physical information.

3. (Original) The method of claim 1, wherein the physical information is included in a document, the document having a substrate that supports the physical information.

4. (Original) The method of claim 3, wherein the physical tag is included on a label that is applied to the document.

5. (Original) The method of claim 1, wherein the physical tag includes a barcode that identifies the public key.

6. (Original) The method of claim 5, wherein the barcode is formed as a glyph code, and wherein the glyph code contains public-key identifying information in a machine-readable graphic.

7. (Original) The method of claim 1, wherein the physical tag carries the public key.

8. (Original) The method of claim 1, wherein the physical tag identifies a location on a digital storage medium, and wherein the location includes the public key.

9. (Original) The method of claim 1, further comprising sending the encrypted digital image from a sender to an address of a recipient, the address being identified by the physical tag.

10. (Original) The method of claim 9, wherein sending includes transmitting a digital signature to the recipient, the digital signature being produced using a private key of the sender and relating to the digital image.

11. (Original) The method of claim 1, wherein digitizing the physical tag is carried out during digitizing the physical information using a single digitizing mechanism.

12. (Previously Presented) The method of claim 11, further comprising removing the digital tag from the digital image before encrypting.

13. (Currently Amended) A method of sending an encrypted image of a document, comprising:

disposing a physical tag on a document, the physical tag having a code that carries a public key;

digitizing the document to create a digital image that includes a digital representation of the code;

reading the digital representation of the code to obtain the public key;

encrypting the digital image with the obtained public key; and

sending the encrypted image to a recipient that holds a private key, the private key forming **an asymmetric public-private pair of cryptography keys** ~~a key pair~~ with the public key.

14. (Original) The method of claim 13, wherein the code includes a barcode.

15. (Original) The method of claim 13, wherein the physical tag carries an address, the address corresponding to the recipient.

16. (Original) The method of claim 13, wherein the code is formed as a glyph code, and wherein the glyph code carries the public key in a machine-readable graphic.

17. (Original) The method of claim 13, wherein the physical tag is included on an adhesive label, and wherein disposing includes applying the adhesive label to the document.

18. (Currently Amended) A device for encrypting an image produced from spatially-distributed physical information, the device comprising:

at least one digitizing mechanism adapted to digitize spatially-distributed physical information to create a digital image, and to digitize a physical tag associated with the physical information to create a digital tag, the digital tag being readable to identify a public key **that is a public member of an asymmetric public-private pair of cryptography keys**; and

a processor operatively connected to the digitizing mechanism and adapted to receive the digital image and digital tag from the at least one digitizing mechanism, to read the digital tag to identify the public key, and to encrypt the image with the identified public key.

19. (Original) The device of claim 18, wherein the physical information is included in a document, the document having a substrate that supports the physical information.

20. (Original) The device of claim 19, wherein the physical tag is included on a label that is applied to the document, the label having a code that identifies the public key.

21. (Original) The device of claim 18, wherein the at least one digitizing mechanism is a single mechanism that digitizes the physical tag during digitizing the physical information.

22. (Original) The device of claim 18, wherein the physical tag carries an address of a recipient, and the processor is adapted to be connected to a network and to send the encrypted image to the address through the network.

23. (Original) The device of claim 18, wherein the physical tag includes a barcode that identifies the public key.

24. (Original) The device of claim 23, wherein the barcode is formed as a glyph code, and wherein the glyph code contains public-key identifying information in a machine-readable graphic.

25. (Original) The device of claim 18, wherein the physical tag carries the public key.

26. (Original) The device of claim 18, wherein the physical tag identifies a location on a digital storage medium, and wherein the location includes the public key.

27. (Currently Amended) A program storage device readable by a processor, tangibly embodying a program of instructions executable by the processor to perform method steps for encrypting an image produced from physical information, comprising:

digitizing spatially-distributed physical information to create a digital image of the information;

digitizing a physical tag associated with the physical information to create a digital tag, the digital tag being readable to identify a public key **that is a public member of an asymmetric public-private pair of cryptography keys**;

reading the digital tag to identify the public key; and

encrypting the digital image with the identified public key.

28. (Original) The program storage device of claim 27, wherein the physical information is included in a document, the document having a substrate that supports the physical information.

29. (Original) The program storage device of claim 28, wherein the physical tag is included on a label that is applied to the document.

30. (Original) The program storage device of claim 27, wherein the physical tag includes a barcode that identifies the public key.